

DECREE
135
of the National Security Authority

dated from 26 March 2009

on the format and method of creating the qualified electronic signature, the method of publishing the public key of the National Security Authority, the conditions of validity for the qualified electronic signature, procedure during the verification and verification conditions of the qualified electronic signature, format of the time stamp and method of creating it, requirements on the source of time data and requirements for keeping time stamp documentation (on the creation and verification of the electronic signature and time stamp) as amended by Decree No. 32/2010 Coll.

In accordance with Art. 4 Para. 4 and 5 Art. 5 Para. 5, Art 9 Para. 2 of Act No. 215 /2002 Coll. on the electronic signature and on the amendment and supplementation of particular acts (hereinafter referred to as ‘the Act’), the National Security Authority (hereinafter referred to as ‘the Authority’) establishes:

Art. 1

Subject of the regulation

This decree regulates

- a) the format and method of creating a qualified electronic signature,
- b) details on the conditions of validity for the qualified electronic signature, the procedure for verifying the qualified electronic signature and the conditions for verifying the validity of the qualified electronic signature,
- c) the method of publishing the Authority's public key,
- d) signature schemes, algorithms and parameters of said algorithms for the creation of the qualified electronic signature,
- e) the format and method of creating time stamps,
- f) requirements for keeping time stamp documentation,
- g) the format, required informational content and method of publishing the signature policy.

Art. 2

Common definitions

For the purposes of this decree,

- a) a signature scheme denotes the unique determination of algorithms for the creation and verification of the qualified electronic signature as well as the parameters of said algorithms,
- b) an approved signature scheme denotes a signature scheme from the index of signature schemes which has been approved and published by the Authority,
- c) a hash function denotes a mathematical transformation which to digital documents of varying length, allocates numbers of a non-zero fixed length specified in advance to enable the verification of the integrity of the digital document from which they were derived by transformation and cannot be used to derive the digital document in reverse,

- d) an approved hash function denotes a hash function specified in the index of approved signature schemes specified in Appendix No. 1,
- e) a digital imprint of the document denotes a number calculated from the document by means of the hash function,
- f) a digital signature of an electronic document denotes the result of the transformation of the digital imprint of the given electronic document by means of the algorithm for the creation of the electronic signature and the private key of the signer,
- g) the identifier of the signature policy is the object identifier uniquely determining the signature policy which is assigned by the Authority; the format and design of the object identifier is established in the international standardisation document,¹⁾
- h) reference time denotes the time which is provided by several of the reference stations,
- i) the issuer of the time stamp (hereinafter referred to as 'the issuer') denotes an accredited certification authority providing a time stamp service,
- j) the relying party denotes the recipient of a time stamp who is relying on its accuracy,
- k) the issuer of the signature policy denotes a subject which defines the specific, technical and procedural rules for the creation and verification of the qualified electronic signature by means of signature policy.

Art. 3

Formats of the qualified electronic signature

(1) The qualified electronic signature shall have a format

- a) without time stamp,
- b) with time stamp,
- c) with the complete information on verification of validity,
- d) archive, or
- e) a combination of formats in accordance with Letters a) to d).

(2) The qualified electronic signature without time stamp contains

- a) the identifier of the signature policy used in creating and verifying the given qualified electronic signature,
- b) signature data which the signer includes in the qualified electronic signature (such as the place and time of the creation of the given electronic signature, the name of the natural person signing for a legal entity and similar),
- c) a digital signature which has been created on the basis of
 1. the digital imprint of the signed document,
 2. the identifier of the signature policy,
 3. data which the signer has included in the electronic signature.

(3) A qualified electronic signature with time stamp has the form of the qualified electronic signature to which a time stamp created on the basis of the given qualified electronic signature by means of the procedure established in Art. 7, Para.2 and 8 and Art. 8 is attached or otherwise logically connected.

(4) A qualified electronic signature with complete information on the verification of validity has the form of the qualified electronic signature with time stamp, to which the complete information on all certificates of public keys needed for the verification of validity of the given

qualified electronic signature is attached, as well as the complete information on the certificate revocation lists or information on the status of the certificates which are decisive in the verification of the validity of the given qualified electronic signature.

(5) An archive qualified electronic signature has the form of the qualified electronic signature with time stamp to which all data needed for the verification of the given archive qualified electronic signature are connected in accordance with Art. 11 Para. 5. The time stamp which is created on the data needed for the verification of the given archive qualified electronic signature, is attached to them.

(6) The Authority publishes valid formats of qualified electronic signatures and the formal specifications thereof on its internet site.

Art. 4 **Signature policy**

(1) The signature policy is a set of rules regulating the creation and verification of qualified electronic signatures.

(2) The subject receiving documents signed with a qualified electronic signature shall determine the signature policy which it accepts. The qualified electronic signature is created by the signer in accordance with the signature policy determined. The validity of the qualified electronic signature is verified by the verifier in consideration of the signature policy which was used to create it.

(3) If a public authority does not have its own issued signature policy, it shall use the signature policy issued by the Authority in verifying the qualified electronic signature of documents received from public authorities and in verifying the qualified electronic signature of documents delivered by a public authority.

(4) The signer and verifier of the qualified electronic signature shall use the same signature policy here.

(5) The format, the required informational content and structure of the signature policy are specified in Appendix 2.

(6) If the signature policy fulfils the requirements according to Section 5, it shall be published on the Authority's internet site and filed in the index of approved signature policies. The signature policy is published in a format which can be processed by machine in accordance with the international standardisation documents.²⁾

(7) The index of approved signature policies contains the name of the signature policy file, hash function, digital imprint of the signature policy file, date of validity, object identifier and field of application of the signature policy.

Art. 5

Creation of the qualified electronic signature

(1) The signer creates the qualified electronic signature of an electronic document using a secure signature creation device³⁾ on the basis of the electronic document and the signer's private key according to any of the approved signature schemes pursuant to Art. 6.

(2) The signer creates the qualified electronic signature with time stamp on the basis of the qualified electronic signature by means of the issuer's time stamp in such a manner that the time stamp issued by an accredited certification authority for the given qualified electronic signature is attached to the qualified electronic signature or is logically connected to the qualified electronic signature for which the time stamp was issued.

(3) The qualified electronic signature with complete information on the verification of validity is created by the signer once the qualified electronic signature with time stamp has been created or by the verifier of the qualified electronic signature with time stamp in such a manner that references to all data needed for the verification of the given qualified electronic signature with time stamp are attached to it in accordance with Art. 11.

(4) The signer creates the archive qualified electronic signature once the qualified electronic signature with time stamp has been created in such a manner that all data needed for the verification of the given qualified electronic signature with time stamp are attached to it in accordance with Art. 11 together with the time stamp which was issued for these data.

Art. 6

Signature schemes for the creation of the qualified electronic signature and time stamp

The index of approved signature schemes, approved algorithms and parameters of approved algorithms for the creation of qualified electronic signatures and time stamps is specified in Appendix No. 1.

Art. 7

Creation and verification of the time stamp

(1) The time stamp policy is a set of rules establishing the usability of the time stamp of a specified circle of time stamp users and the application class with the common security requirements³⁾. The time stamp policy is created by the users of the time stamps and the issuers of the time stamps.

(2) A legal entity or natural person applying for the creation of a time stamp (hereinafter referred to as 'the applicant') shall send an application for the creation of a time stamp to the time stamp issuer. The application shall contain the digital imprint of the document, created using the approved hash function, on which the time stamp is to be created.

(3) If the application meets the requirements established in Section 2 and there are no restrictions on the creation of the time stamp on the part of the issuer pursuant to Art. 9 Para. 4, the issuer shall create the time stamp on the submitted digital imprint of the document using the

secure device for creating time stamps and the time source and send it to the applicant by the time established by the time stamp policy.

(4) If the application for the creation of a time stamp does not meet the requirements established in Section 2 or the restrictions on the creation of time stamps pursuant to Art. 9 Para. 4 have occurred at the issuer; the issuer shall not create the time stamp on the submitted digital imprint of the document and shall inform the applicant of this circumstance and the reason for it by the time established by the time stamp policy.

(5) The verification of the validity of the time stamp is conducted by the relying party on the basis of the time stamp and document for which the given time stamp was created and the time stamp policy to which the given time stamp relates.

The time stamp is valid if

- a) it is in compliance with the time stamp policy used,
- b) the electronic signature of the issuer's time stamp is valid.

(6) The format of the application for the creation of the time stamp, the format of the time stamp and the format of the response to the application for the creation of the time stamp are published in the Authority's website.

Art. 8

Requirements for the source of the time data for the time stamp

The source of the time date which the issuer uses to create the time stamp must meet the following requirements:

- a) the source of the time data is synchronised with the reference time source with the declared accuracy,
- b) the calibration of the time data source is maintained in such a manner as to ensure that deviations exceeding the range of the declared accuracy do not take place,
- c) the time data source is protected from danger which may cause undetectable changes to the time source data leading to deviation exceeding the range of calibration,
- d) the detection of cases, in which the time data to be specified in the time stamp deviates from the synchronisation with the reference source time, is ensured; the issuer must inform the relying parties of such cases,
- e) the issuer conducts the synchronisation of the time data source in the event a correction second is issued on the basis of the reference time administrator's announcement,
- f) the issuer conducts a change in which the correction second is set at the last minute of the day on which the change is planned; the issuer creates a record on the precise time with the declared accuracy of the execution of said change.

Art. 9

Requirements for the time data for the time stamp

(1) The issuer shall create time stamps using a reliable method. The time stamps must contain correct time data.

(2) For the creation of time stamps the issuer shall use at least one time source, providing

reliable time data, which meets the requirements specified in Art. 8.

(3) Time data which the time stamp contains are demonstrably derived from at least one of the reference time values.

(4) If the source of the time data does not achieve the required accuracy, that is, if it deviates from the reference time source by more than is specified in the operational order of the time stamp issuer, the issuer shall not issue the time stamp.

Art. 10

Documentation of time stamps

(1) All information on the provision of the service of issuing time stamps shall be recorded and stored in accordance with the time stamp policy.

(2) When issuing time stamps, the issuer shall keep:

- a) an index of time stamps created by the issuer in which the time stamp is stored from its creation for a time period specified by the time stamp policy used by the issuer,
- b) records of extraordinary incidents in the system used in the management of the time stamps,
- c) records of important events in the environment of the time stamp issuer, management of cryptographic keys and synchronisation of the time source including precise time data.

Art. 11

Verification of validity of the qualified electronic signature

(1) The qualified electronic signature is valid if

- a) the digital signature contained in the qualified electronic signature is valid,
- b) the qualified electronic signature of an electronic document was created in accordance with the specified signature policy valid at the time of its creation,
- c) all certificates in the certification path are valid.

(2) The qualified electronic signature with time stamp is valid if the following can be demonstrated clearly:

- a) the validity of the qualified electronic signature pursuant to Sections 1 and 5 at the time from the valid time stamp of the qualified electronic signature,
- b) the validity of the time stamp of the qualified electronic signature pursuant to Art. 7 Para. 5.

(3) The qualified electronic signature with the complete information on verification of validity is valid if:

- a) the information on the verification of the qualified electronic signature is available and complete pursuant to Section 5,
- b) the qualified electronic signature with time stamp is valid pursuant to Section 2.

(4) The archive qualified electronic signature with time stamp is valid if the following can be demonstrated clearly:

- a) the validity of the time stamp pursuant to Art. 7 Para. 5 which was created on the basis of data pursuant to Sections 1 and 5,

- b) the completeness of the information for the verification of the qualified electronic signature,
- c) the validity of the qualified electronic signature with time stamp pursuant to Section 2.

(5) The verifier shall use the following to verify the validity of the qualified electronic signature

- a) the electronic document for which the qualified electronic signature was created,
- b) the qualified electronic signature of the electronic document,
- c) the public key from a valid qualified certificate corresponding to the private key, by means of which the qualified electronic signature was created,
- d) the signature policy in which the object identifier is specified in the qualified electronic signature or the valid object identifier of the accepted signature policy from the index pursuant to Art. 4 Para. 7,
- e) the valid public keys corresponding to the private keys, by means of which the signatures of the certificates and certificate indexes were created in the certification path,
- f) the certificate revocation lists for all certificates in the certification path, potential information on the status of certificates in the certification path obtained from the confirmation of the existence and validity of the certificate.

Art. 12

The Authority's public key

(1) The Authority's public key is a public key corresponding to the Authority's private key. By means of the Authority's private key, the Authority

- a) creates the electronic signature of the certificates of the public keys of the accredited certification authorities,
- b) creates the electronic signature of the certificate of its own public key,
- c) creates the electronic signature of the certificate revocation list issued by the Authority.

(2) The Authority publishes its public key by publishing the certificate of the Authority's public key in the press and on the Authority's internet site. The Authority may also publish its public key by other means.

(3) The Authority issues a new public key of the Authority 30 days before the expiration of the Authority's current public key and publishes it by the means specified in Section 2.

Art. 13

Transitional provisions

(1) Certified products for the qualified electronic signature utilising signature schemes and asymmetrical RSA cipher algorithm with a parameter of MinModLen 1024 bits or lower and certified products utilising the SHA1 hash function can be used until the expiration of the validity period of the product certification, but no later than 31 December 2009.

(2) Products for the qualified electronic signature utilising the RSA algorithms certified after 1 January 2009 must use the RSA algorithm with the MinModLen 2048 parameter. Products for the qualified electronic signature utilising the SHA algorithm certified after 1 January 2009 must

use the hash function from the SHA-2 array or another of the recommended hash functions with a period of validity exceeding 31 December 2009.

(3) Certificates for the provision of accredited certification services utilising the SHA1 hash function and RSA algorithm with MinModLen parameter lower than 2048 bits can be used for verification until 31 December 2010.

(4) The SHA1 hash function and RSA algorithm with the MinModLen parameter lower than 2048 bits can be used until 31 December 2010 for the provision of accredited certification services for issuing the certificate revocation lists and confirmation of the existence and validity of qualified certificates.

(5) It is recommended to proceed in accordance with the international standardisation document⁴⁾ when selecting algorithms.

Art. 13a

Transitional provisions for amendment effective from 1 February 2010

Certified products for the qualified electronic signature utilising signature schemes with the RSA algorithm with the parameter of MinModLen 1024 bits and certified products utilising the SHA1 hash function defined in Appendix No.1 which could have been used until 31 December 2009, may be used until 31 December 2010.

Art. 14

Annulling clause

National Security Authority Decree No. 537/2002 Coll. on the format and method of creating the qualified electronic signature, method of publishing the Authority's public key, verification procedure and verification conductions of the qualified electronic signature, time stamp format and method of its creation, requirements on the time data source and requirements on keeping time stamp documentation (on the creation and verification of the electronic signature and time stamp) is repealed.

Art. 15

Final provision

This Decree has been adopted in accordance with the applicable legal act of the European Community⁵⁾ under notification number 2008/0528/SK.

Art. 16

Period of validity

This Decree shall enter into force on the day of its declaration.
Decree No. 32/2010 Coll. entered into force on 1 February 2010.

**Appendix No. 1
to Decree No. 135/2009 Coll.**

Signature schemes

Signature scheme is formed by a sequence of designations defined in this Appendix, separated by a semicolon, where the designation of the signature algorithm comes first.⁴⁾

Hash functions

| Hash function designation | Name used | Validity period |
|----------------------------------|------------------|------------------------|
| 1.01 | sha1 | Until 31 December 2010 |
| 1.02 | ripemd160 | Until 31 December 2010 |
| 1.03 | sha224 | Not specified |
| 1.04 | sha256 | Not specified |
| 1.05 | Whirlpool | Not specified |
| 1.06 | sha384 | Not specified |
| 1.07 | sha512 | Not specified |

Signature algorithms

| Signature algorithm designation | Signature algorithm | Key generation algorithms | Signature algorithm according to minimum size of parameters along with its usage period |
|---------------------------------|---------------------|---------------------------|--|
| 2.01 | rsa | rsagen1 | MinModLen=1024, ErrProb= 2^{-80} , SeedEntropy/EntropyBits=80 - until 31 December 2010 MinModLen=2048, ErrProb= 2^{-100} , SeedEntropy/EntropyBits=100 |
| 2.02 | dsa | dsagen1 | pMinLen=1024, qMinLen= 160, ErrProb= 2^{-80} , SeedEntropy/EntropyBits=80 – until 31 December 2010 pMinLen=2048, qMinLen=224, ErrProb= 2^{-100} , SeedEntropy/EntropyBits=100 |
| 2.03 | ecdsa-Fp | ecgen1 | pMinLen=-, qMinLen=160, r0Min=104, MinClass=200, ErrProb= 2^{-80} , SeedEntropy/EntropyBits=80 – until 31 December 2010 pMinLen=-, qMinLen=224, r0Min=104, MinClass=200, ErrProb= 2^{-100} , SeedEntropy/EntropyBits=100 |
| 2.04 | ecdsa-F2m | ecgen2 | mMin=-, qMinLen=160, r0Min=104, MinClass=200, ErrProb= 2^{-80} , SeedEntropy/EntropyBits=80 – until 31 December 2010 mMin=-, qMinLen=224, r0Min=104, MinClass=200, ErrProb= 2^{-100} , SeedEntropy/EntropyBits=100 |
| 2.05 | ecgdsa-Fp | ecgen1 | pMinLen=-, qMinLen=160, r0Min=104, MinClass=200, ErrProb= 2^{-80} , SeedEntropy/EntropyBits=80 – until 31 December 2010 pMinLen=-, qMinLen=224, r0Min=104, MinClass=200, ErrProb= 2^{-100} , SeedEntropy/EntropyBits=100 |
| 2.06 | ecgdsa-F2m | ecgen2 | mMin=-, qMinLen=160, r0Min=104, MinClass=200, ErrProb= 2^{-80} , SeedEntropy/EntropyBits=80 – until 31 December 2010 mMin=-, qMinLen=224, r0Min=104, MinClass=200, ErrProb= 2^{-100} , SeedEntropy/EntropyBits=100 |

Algorithms for generation of key pairs

| Key generator designation | Name used | Signature algorithm | Random number generation method | Random generator parameters |
|---------------------------|-----------|-----------------------|---------------------------------|-----------------------------|
| 3.01 | rsagen1 | rsa | trueran | EntropyBits |
| 3.02 | dsagen1 | dsa | trueran or pseuran | EntropyBits or SeedEntropy |
| 3.03 | ecgen1 | ecdsa-Fp, ecgdsa-Fp | trueran or pseuran | EntropyBits or SeedEntropy |
| 3.04 | ecgen2 | ecdsa-F2m, ecgdsa-F2m | trueran or pseuran | EntropyBits or SeedEntropy |

Completion methods (padding)

| Padding designation | Name used | Random number generation method | Random generator parameters |
|---------------------|-----------------|---------------------------------|-----------------------------|
| 4.01 | emsa-pkcs1-v1.5 | - | - |
| 4.02 | emsa-pkcs1-v2.1 | - | - |
| 4.03 | emsa-pss | trueran/pseuran | MinSaltEntropy |
| 4.04 | iso9796ds2 | trueran/pseuran | MinSaltEntropy |
| 4.05 | iso9796-din-rn | trueran/pseuran | MinSaltEntropy |
| 4.06 | iso9796ds3 | - | - |

Random number generation method

| Generation method designation | Name used | Random generator parameters |
|-------------------------------|-----------|-----------------------------|
| 5.01 | trueran | EntropyBits |
| 5.02 | pseuran | SeedEntropy |

SIGNATURE POLICY

1. The structure of the signature policy consists of the cover of the signature policy, the signature policy data and the rules for signature verification.
2. The cover of the signature policy contains the hash algorithm identifier, data on the signature policy and an optional digital imprint of the signature policy data.
3. The signature policy data most notably contain the:
 - 3.1 Object identifier (OID),
 - 3.2 Date of issue,
 - 3.3 Name of issuer,
 - 3.4 Area of application,
 - 3.5 Signature verification rules, which most notably contain the:
 - 3.5.1 Validity period,
 - 3.5.2 Generally binding rules,
 - 3.5.3 Specific commitments which may supplement the generally binding rules on the basis of identification by means of the object identifier which the signer has included in the signed attributes of the signature. The text information which the application must present to the signer and verifier must be associated with the specified object identifier,
 - 3.6 The rules for the signer and verifier on the obligations of stating and verifying the attributes of the signature and certificate,
 - 3.7 Rules for the use of certificates of the root certification authorities for the signer and for verifying time stamps with a defined maximum period in which the information on the revocation of the certificates will be published,
 - 3.8 Permitted algorithms and minimum key length.

¹⁾ ISO/IEC 6523.

²⁾ ETSI TR 102 272 Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies or ETSI TR 102 038 TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies.

³⁾ Decree of the National Security Authority No.134/2009 Coll. stipulating the details on requirements for secure devices for the creation of time stamps and requirements on products for the electronic signature (on electronic signature products)

⁴⁾ ETSI TS 102 176-1: Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.

⁵⁾ Directive 98/34/EC of the European Parliament and of the Council on a procedure for the provision of information in the field of technical standards and regulations (OJ L 204, 21.7.1998, special edition of the OJ in chap. 3/volume 20) as amended.